Platform Security

Geoffrey Strongin

Platform Security Architect

Advanced Micro Devices, Inc.

Advanced Development Lab

January 23, 2001

Outline

- Introduction
- Platform Security Background
- Key Technologies
- Trusted Client PC Systems
- Wave Systems Work
- Summary
- Future requirements

Introduction

- **Platform Security is:**
  - A: Not really our job
  - B: A serious problem we have to solve
  - C: A big opportunity
  - D: All of the above
- **The Answer is D: All of the above**
  - A: True because much of platform security is the responsibility of OS and application vendors
  - B: True because without hardware, software alone can not currently achieve complete security
  - C: True because removing limitations on PC usage ensures PCs are not marginalized

Security is Not Our Job

- The OS *is* responsible for resource management
- What about all the software security products? Don't they address the issue?
- Applications that need it, build in their own security
- Protocols like SSL and IPSec solve the problem
- Encryption is available to everyone
- Smart cards solve the problem

Security is a Serious Issue

- **The hot buttons depend on where you sit**
  - Corporations: Big targets, Big resources
    - Viruses, worms, break-ins,web site vandalism, theft of data, DoS, lower TCO
  - Small business: Smaller target, Smaller resources
    - Same concerns as the big boys
  - Individuals: Small target, No resources
    - Loss of anonymity, loss of privacy, credit card fraud, viruses, worms, Trojans, identity theft
  - Merchants
    - Credit Card Fraud, reputation
    - Recent report: Fraud at on-line merchants is 60X that of brick and mortar companies
  - Content Providers
    - Theft of content– Not just music, may also be software.
  - Financial Institutions
    - Fraud

Platform Security is a Big Opportunity

- **Meeting the needs of customers is always good business**
- **There is more to the opportunity than just this:**
  - From the start, PCs have been untrustworthy
  - We have come to accept this without challenge
  - Consequently, the PC's utility is decreased
  - Improving the trust in PCs ✍ More applications for PCs
    - » Example: Conditional access for cable TV
  - New content distribution models
  - Service and content subsidies for trusted platforms
    - » Get the beneficiaries to pay for the solution

Why is Hardware Needed?

- **A house needs a strong foundation**
  - A hardware foundation of trust is needed
  - Who watches the watcher?
- **Hardware help is needed to keep secrets**
- **Without it, successful attacks are probable after enough time has elapsed**
- **Without good hardware binding, successful attacks can be distributed over the net**

Issues Specific to PC's

- **Privacy**
  - A lighting rod
  - An issue because of the outcry over previous implementations
  - Some (unique) system ID is required to enable remote trust
  - Key issue is that unique ID must be "tunneled" to guarantor
  - Strong user authentication can (perversely) protect privacy
- **Security**
  - All SW is suspect without a hardware foundation of trust
  - Platform firmware must be protected
  - Strong user authentication critical to many applications
    - Two-factor authentication is generally regarded as safe
  - Opaque processing with secrets is required
- **Ownership (Digital Rights Management)**
  - Trusted & opaque processing are required
  - Secret storage is required

Trusted Client PCs

- **Problem statement: The PC is not Trustworthy**
  - Not a controversial statement in the security world
  - Fixing the problem will take (lots of) time
- **A solution is available now**
  - Add to PCs an internal “trusted engine”
  - Simple enough to be trustworthy
  - Some hardware basis to ensure a solid “root of trust”
  - Simplest view: Embed a programmable smart card in the system
  - Goes back to PC basics: Provide the platform, not the applications

Trusted Client Technologies

- **Cryptography**
  - Symmetric and asymmetric ciphers, and cryptographic hash functions
  - Digital signatures, etc.
- **Tamper Resistant (opaque) Execution Environment**
  - No leaks of (secret) information during processing
- **Good random number generation is important**
  - Mostly for key Generation
- **Good Security Protocols**
  - Authentication, authorization, etc.
  - This is often the weak link

Security vs. Privacy

- **There is a natural tension between privacy and security**
  - Local verification of credentials is the best
  - Trusted local system is needed
  - Trusting the local system implies we authenticate it!
  - Authentication requires credentials
  - We are back where we started
- **The solution is to separate the two sequences**
  - Authenticate the trusted system to an infrastructure
  - Authenticate the individual to the system

Authentication with Privacy

- **Authenticating a system to a (remote) infrastructure requires proof that a secret is known**
  - PKI provides one answer using certificates
  - Alternatively, a shared secret can be used
  - The infrastructure must trust (define) the process of creating valid secrets
- **The infrastructure for authenticating client systems should NOT use this information for any other purpose**
  - This is a key requirement to avoid “triangulation”
- **There are significant legal implications that apply to the authentication infrastructure**

Security vs. Privacy cont.

- **The authentication infrastructure for trusted clients should:**
  - Be used only to authenticate client side characteristics that are relevant to the level of trustworthiness
    - » For example what is the FIPS level…
  - Provide an assertion to 3rd parties about the system without revealing any persistent platform ID
  - Not know anything about the owner/user
  - Provide the assertion under clear and agreed upon contractual terms

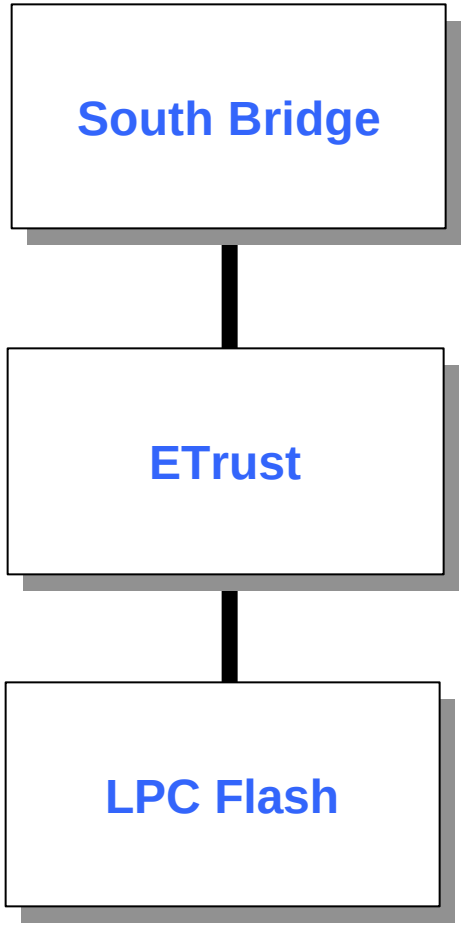
Infrastructure Legal Issues

- **Liability allocation is essential**
  - No system is 100% secure
  - To get close costs lots of $
  - The system must be designed to accept some “leaks”
  - Who pays when this happens must be clear
- **Without liability allocation relying parties would be free to go after deep pocket targets**
  - Relying parties must accept most of the liability
  - Fraud should be about the only exception

AMD and Wave Systems: Working Together

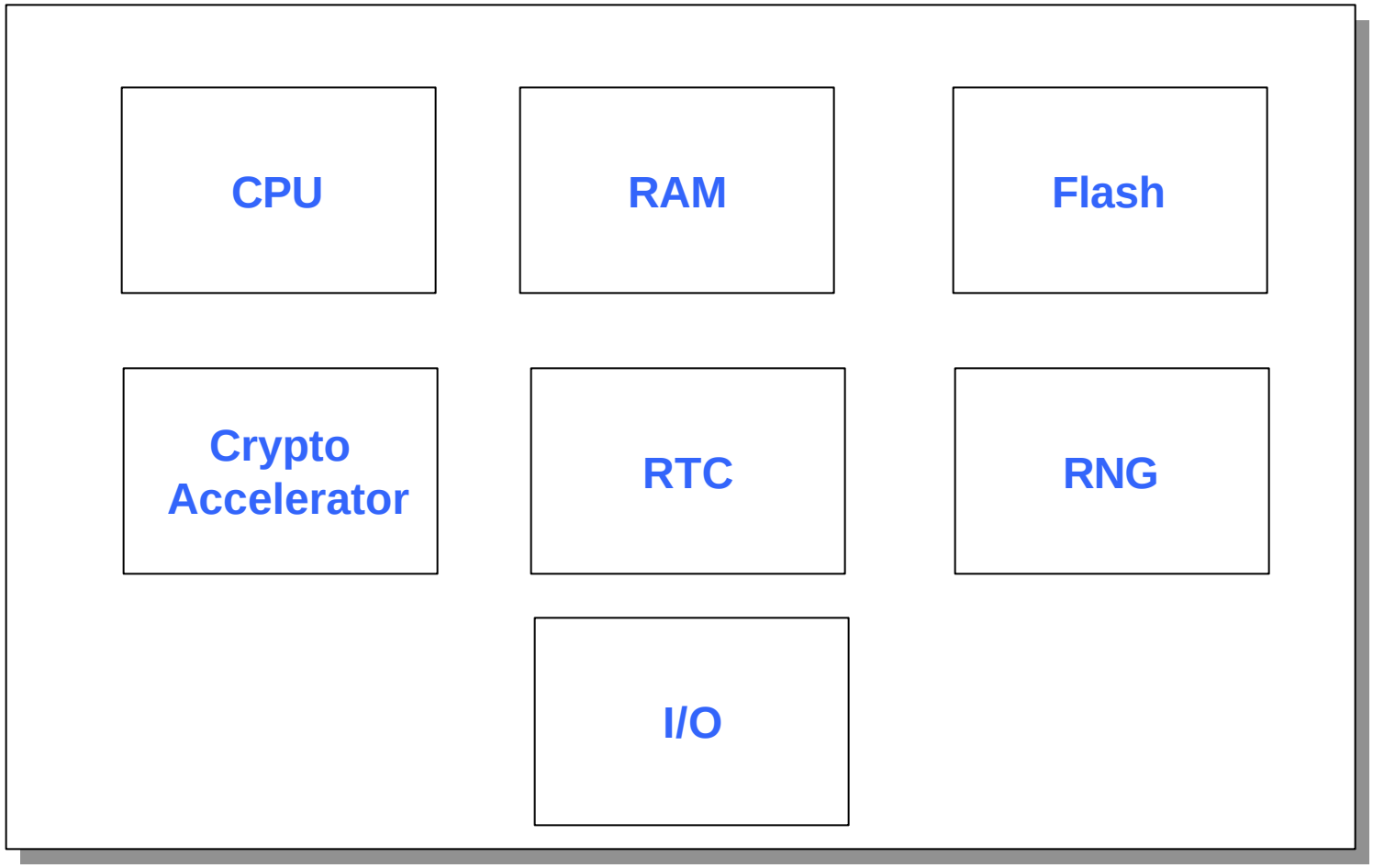
- **Wave Systems has been developing Trusted Client Technology for 10 years**
  - Wave has developed the EMBASSY architecture
  - This is both an ECommerce Infrastructure with an ETrust component
  - AMD is working with Wave Systems to perform the platform engineering to make it easy to integrate the Embassy ETrust into the PC platform
  - OEMs may have this as an option if they choose to deploy Trusted Client PCs

ETrust in a System



LPC/LPC Bridge

ETrust - A System on a Chip



ETrust in the Platform

- **Provides a rock solid hardware root of trust**
  - System BIOS can be verified by the ETrust
  - System BIOS updates can be authenticated by ETrust
  - ETrust has bus master capability on LPC
- **Provides Trusted Client Capabilities**
  - Ties to an authentication infrastructure
  - Can accept “applets” developed by Wave and 3rd Parties
  - Is an open environment
- **Adds BOM Cost**

ETrust Cost Issues

- **AMD understands the cost pressures OEMs face**
  - No one wants to pay for “security”
  - Value of “Trustworthiness” is not determined
- **A Trusted Client PC is a revenue opportunity**
  - Razors/razor blades
  - Various business models exist for cost recovery
  - The key is to get the true beneficiaries to pay
    - » Content providers
- **OEMs interested in Service Revenue**
- **Talk to Wave Systems for specifics**

Call to Action

- **Begin laying the groundwork for deploying Trustworthy PCs**
  - Done right, this can be a strong motivator to stimulate a turnover in the installed base
- **Work across internal marketing/engineering boundaries**
  - Services divisions need to help platform divisions justify additional cost adder to enable service revenue
  - Opportunity is planned to be overall increased margins

Contact me @ Geoffrey.Strongin@amd.com for more details on the Etrust platform for PCs